NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Water filtration plant in Columbia Heights evacuated after chemicals mixed; no injuries.** A water treatment facility in Columbia Heights, Minnesota, was evacuated after two chemicals were accidentally mixed together and caused a reaction February 14. The assistant fire chief said workers notified the Columbia Heights Fire Department that hydrochloric acid and caustic soda had been combined at the plant. When mixed, the two chemicals cause excessive heat. The heat caused the building's sprinkler system to go off. All employees were immediately evacuated. The assistant fire chief did not know how the chemicals were incorrectly mixed. The plant is the City of Minneapolis' water filtration plant. Minneapolis officials said drinking water was never at risk of contamination and that the city's tap water is safe to drink. Source: http://www.therepublic.com/view/story/09763953dc2c4654a87474294e4a46d4/MN--Water-Treatment-Evacuation/

National

Nothing Significant to Report

International

Inspections reveal serious flaws at 11 Bulgarian dams. The ongoing inspection of the condition of dams located all over Bulgaria has so far identified serious problems at 11 facilities of a total of 140 checked, according to the minister of economy, energy and tourism. After a meeting February 15, he explained the problematic dams were located in five districts — one in Kardzhali, one in Smolyan, two in Montana, three in Pazardzhik, and three in Sliven. Like the Elena dam, which was subjected to a controlled draining February 13 over a risk of failure, the majority of the faulty reservoirs have non-functioning spillways and release gates, the CEO of the national power grid operator, NEK, concluded. He warned the release gates of the dams needed urgent repairs and the facilities had to be equipped with emergency gates. Source: http://www.novinite.com/view_news.php?id=136693

Monsanto guilty of chemical poisoning in France. A French court February 13 declared U.S. biotech giant Monsanto guilty of chemical poisoning of a French farmer, a judgment that could lend weight to other health claims against pesticides. In the first such case heard in France, a grain grower said he suffered neurological problems including memory loss, headaches, and stammering after inhaling Lasso weedkiller in 2004. He blames the agri-business giant for not providing adequate warnings on the product label. The court in Lyon sought an expert opinion of losses to establish damages. Previous health claims from farmers have foundered because of the difficulty of establishing clear links between illnesses and exposure to pesticides. The grain

grower joined with other farmers suffering from illness to set up an association last year. The agricultural branch of the French social security system said since 1996, it has gathered about 200 reports a year of farmers' claiming they were sickened by pesticides. But only 47 cases in the past 10 years have been recognized as due to pesticides. Source: http://www.reuters.com/article/2012/02/13/france-pesticides-monsanto-idUSL5E8DD5UG20120213

Banking and Finance Industry

FTC action leads to ban on alleged mortgage relief scammers who harmed thousands of consumers. At the request of the Federal Trade Commission (FTC), a U.S. district court February 14 put the mortgage relief business permanently off limits to marketers who allegedly charged thousands of consumers up to $2,600 each, based on bogus promises to provide loan modifications that would make mortgages more affordable. According to the FTC, the scheme caused consumer losses of nearly $19 million. All but two of the defendants settled with the agency, while the two other corporate defendants received default judgments. The FTC alleged the defendants used direct mail, the Internet, and telemarketing to target homeowners. The defendants typically asked for half of the fee up-front, falsely claiming a success rate of up to 100 percent, according to the complaint. They deceptively claimed they could prevent foreclosure, that they were affiliated with or approved by consumers' lenders, and that they would refund consumers' money if they failed to deliver promised services, according to the FTC. They told consumers not to contact lenders and to stop making mortgage payments, claiming that falling behind on payments would demonstrate hardship, the FTC alleged. The complaint charged U.S. Mortgage Funding, Inc., Debt Remedy Partners Inc., Lower My Debts.com LLC, and four individuals with violating the FTC Act and the FTC's Telemarketing Sales Rule. The court orders ban all the defendants from providing mortgage and debt relief services and telemarketing. Source: http://www.ftc.gov/opa/2012/02/usmortgage.shtm

Chemical and Hazardous Materials Sector

EPA sets new rules for emissions from PVC production. The Environmental Protection Agency (EPA) February 14 set stringent emissions limits for industrial plants that manufacture polyvinyl chloride, a ubiquitous plastic commonly known as PVC. The new rule comes two years after a settlement between three activist groups and the EPA. The Sierra Club and two community groups in Louisiana filed a lawsuit in 2008 to force the agency to establish limits for several harmful pollutants at the nation's 17 vinyl-producing plants, including four in Texas. The rule sets limits for three air toxics — vinyl chloride, chlorinated di-benzo dioxins and furans, and hydrogen chloride. The previous rule only covered vinyl chloride, a known carcinogen. The EPA estimates the tougher standard will reduce emissions by 262 tons annually, with the cost of compliance at $4 million a year after an initial capital investment of $18 million. The Vinyl Institute, an industry group based in Virginia said the rule's economic impact could be as high as $100 million, based on the EPA's earlier proposal. Source: http://www.chron.com/news/houston-texas/article/EPA-sets-new-rules-for-emissions-from-PVC-3324417.php

Committee leaders express concern over EPA policy that could compromise chemical facility security. U.S. House Energy and Commerce Committee leaders sent a letter February 10 to the Environmental Protection Agency (EPA) administrator expressing concern over a recent announcement that they claimed could compromise sensitive data and make U.S. chemical manufacturing facilities more susceptible to terrorist attacks. They voiced strong opposition to the EPA's decision to re-establish Internet access to manufacturers' non-Off-site Consequence Analysis sections of the Risk Management Plan database, sections that contain lists of covered chemicals used, preventative measures, and the location in a plant where those chemicals are used. The leaders asked the administrator to reverse the decision. In the letter, they argued publishing the data could provide "a virtual terrorist roadmap into a chemical facility." They added: "This is why EPA decided to remove all Risk Management Plan data from the Agency website in the fall of 2001." Source: http://energycommerce.house.gov/news/PRArticle.aspx?NewsID=9292

Industry progressing in voluntary effort to reduce toxic chemicals. The U.S. Environmental Protection Agency (EPA) released February 10 interim results of a voluntary effort by eight chemical manufacturers to reduce emissions and use of long-chain perfluorinated chemicals (LCPFCs), including perfluorooctanoic acid (PFOA). Used in hundreds of manufacturing and industrial applications, LCPFCs are toxic, persistent in the environment worldwide, and can accumulate in people. The agency's 2010/15 PFOA Stewardship Program was established in 2006 in partnership with eight companies. The program set a goal of reducing facility emissions and product content of PFOA and related chemicals on a global basis by 95 percent, no later than 2010, and to work toward eliminating emissions and product content by 2015. Daikin America, Inc., DuPont, 3M/Dyneon, and Solvay Solexis met the program's intermediate goal of a 95 percent reduction in emissions and product content by 2010, the EPA said. It noted 150 replacement chemicals have been developed. The eight manufacturers informed the EPA they are on track to phase out LCPFCs by the end of 2015. Source: http://news.thomasnet.com/companystory/Voluntary-Effort-Makes-Progress-in-reducing-LCPFCs-PFOA-609677

EPA moves to prevent fuel spills on farms. The Environmental Protection Agency (EPA) is requiring farmers with 10,000 gallons of fuel storage or more to come up with engineer-certified fuel spill containment facilities, the Billings Gazette reported February 10. Smaller farms with storage below the 10,000 mark but more than 1,320 gallons have to complete a self-designed plan for containing fuel spills. Farm fuel spills have been only softly regulated by the EPA, but the agency is bringing more focus on spills out of concern for water quality and levying fines of more than $1,000 for major noncompliance. The Natural Resources and Conservation Service (NRCS) began offering Montana farmers help with the plan design and construction costs. The NRCS is getting involved because it would like plans that not only address risks to rivers and streams, but also groundwater.Source: http://billingsgazette.com/news/state-and-regional/montana/epa-moves-to-prevent-fuel-spills-on-farms/article_0325148a-cd86-57b8-9bff-c41fec1102bc.html

Commercial Facilities

Nothing Significant to Report

Communications Sector

(Kansas) **Copper thief pleads guilty to damaging utility.** A Kansas copper thief is looking at a possible 20 years in prison for pulling down power poles to get at the wiring, the Kansas City star reported February 13. His action also caused a southeastern Kansas radio station to go off the air for several hours. He was finally stopped by an armed property owner who caught him trying to steal a copper coupling from his propane tank, prosecutors said. He pleaded guilty February 13 to one count of damaging an energy facility. A second charge of obstructing the national Emergency Alert System by putting the radio station out of commission was dropped. The man stole copper wire September 7 by pulling down an electrical pole belonging to the Heartland Rural Electric Company. That caused a second pole also to fall. And that affected radio station KKOW in Pittsburg, Kansas, whose transmission tower was at the site. Source: http://www.kansascity.com/2012/02/13/3427390/copper-thief-pleads-guilty-to.html

Critical Manufacturing

NHTSA recall notice - Navistar IC Bus and International models traction relay valves. Navistar announced February 16 that it recalled 18,959 model year 2012-2013 IC Bus HC and International 9400, and certain model year 2011-2013 International Durastar, Payster, Workstar, Transtar, Lonestar, Prostar, 9200, and 9800, and certain model year 2013 International 9900 vehicles manufactured from December 2, 2010, through January 26, 2012 and equipped with Bendix ATR-6 traction relay valves. In extremely cold conditions these valves may develop internal leakage. Leakage can lead to air pressure being delivered to affected primary or secondary brakes, causing continuous brake application. Unexpected continuous brake application can cause the brakes to overheat and lead to a fire. Unexpected continuous brake application can also cause the driver to lose control of the vehicle. Also, the brakes may be applied without illuminating the brake lights, failing to give proper warning to other drivers. Navistar will notify owners, and dealers will provide a temporary repair until Bendix develops a permanent remedy. The safety recall is expected to begin on or before April 6. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V052000&summary=true&prod_id=1170772&PrintVersion=YES

STIHL recalls chain saws due to risk of injury. The U.S. Consumer Product Safety Commission, in cooperation with STIHL Inc., February 14 announced a voluntary recall of about 3,000 STIHL MS 391 chain saws. Consumers should stop using recalled products immediately unless otherwise instructed. The flywheel on the chain saw can crack causing parts of the flywheel to separate and strike users or bystanders, posing a risk of injury. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12108.html

Fire control panels recalled by Bosch Security Systems Corp. due to alarm failure posing a fire hazard. The Consumer Product Safety Commission, in cooperation with Bosch Security Systems Corp., February 15 issued a recall of about 330 fire alarm control panels. Consumers should stop using the product immediately unless otherwise instructed. On all systems, when the alarm verification feature of the system is turned on, the control panel can fail to sound an alarm if a fire occurs. In addition, on systems with 50 or more reporting stations, a delay in sounding an alarm and reporting a fire may occur if the loop for the alarm system is broken. All distributors and installers are being sent two technical bulletins. One provides instructions for how to implement a software change that will correct the verification feature. The second contains instructions for how to handle warnings from affected systems with 50 or more stations. Those who have not received the bulletins should contact Bosch. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12721.html

DEFENSE/ INDUSTRY BASE SECTOR

Problems with motor slow U.S. AMRAAM buys. The Pentagon slowed down its purchases of the new AIM-120D version of the Advanced Medium Range Air-to-Air Missile (AMRAAM) because of problems with producing its rocket motors, the U.S. Air Force's top acquisition official said February 14. "They're behind on the delivery of the missile," he said of the Raytheon-produced system. The Air Force reduced the number of missiles it is buying to 113 units, down from 138 the year before. Overall, the Pentagon plans to spend $423 million on continued production of the active radar-guided AIM-120D for a total of 180 missiles, including Navy and Marine Corps buys. The official said the quality of the missiles already delivered is "fine," but the weapons cannot be produced in quantity due to a high rejection rate for the rocket motors being built. However, the Pentagon must have the new AMRAAM variant. The next-generation Joint Dual-Role Air Dominance Missile, which would have replaced the AMRAAM and the AGM-88 High Speed Anti-Radiation missile, which is used to suppress enemy air defenses, was terminated because it was unaffordable. Source: http://www.defensenews.com/article/20120214/DEFREG02/302140011/Problems-Motor-Slow-U-S-AMRAAM-Buys?odyssey=tab|topnews|text|FRONTPAGE

(Pennsylvania) **Anonymous movement claims hacking attack on U.S. tear gas company.** The Web site of a Jamestown, Pennsylvania-based company whose tear gas was used against demonstrators in Egypt is the latest to be broken into by the Anonymous movement, the hackers claimed February 14. In a statement posted to the Internet, the hackers accused Combined Systems of being war profiteers who sell "mad chemical weapons to militaries and cop shops around the world." Anonymous said it targeted Combined Systems because it was supplying weaponry used to "to repress our revolutionary movements." The hackers also claimed to have stolen and published personal information belonging to clients and employees of the firm. Allegedly intercepted e-mails were pasted onto the bottom of the statement; one of them appeared to be a warning that Combined Systems' site was sabotaged. Neither the hackers' claims nor the authenticity of the e-mails could be immediately verified, although the Web site was down February 14. The company sells a variety of security wares, including aerosol grenades, sprays, and handcuffs. Source:

http://www.usatoday.com/tech/news/story/2012-02-14/anonymous-hacks-tear-gas/53087858/1

Emergency Services

Nothing Significant to Report

Energy

Gas well inspections to be required after fracking, U.S. Secretary of the Interior says. Natural-gas drillers will be required by U.S. rules to inspect their wells after hydraulic fracturing on public land to ensure the safety of drinking-water supplies, the Secretary of the Interior said February 14. In the coming weeks, the Department of the Interior will propose standards under which companies such as Chesapeake Energy Corp. and Exxon Mobil Corp. must disclose the chemicals in the mixture injected underground to free trapped gas, demonstrate the well is not leaking, and check the work after fracking. The agency will also require that drilling on federal land meets guidelines for handling fracking water that returns to the surface after being injected into the rock to make sure streams are not contaminated. Source: http://www.bloomberg.com/news/2012-02-14/gas-well-inspections-to-be-required-after-fracking-salazar-says.html

Food and Agriculture

65 Campylobacter infections now tied to raw milk dairy. An additional five cases have bumped up the number of confirmed Campylobacter infections linked to raw milk produced by the Your Family Cow dairy in Chambersburg, Pennsylvania, to 65, the Pennsylvania Department of Health reported February 13. The latest breakdown of illnesses by state are: Pennsylvania (56); Maryland (4), West Virginia (3) and New Jersey (2). Unpasteurized milk in two unopened bottles from the dairy tested positive for the outbreak strain, according to Maryland health officials. After making some improvements to its equipment, the Family Cow dairy was cleared by the Pennsylvania Department of Agriculture to resume selling raw milk the week of February 6. Source: http://www.foodsafetynews.com/2012/02/65-campylobacter-infections-now-tied-to-raw-milk-dairy/

Government Sector (including Schools and Universities)

Stratfor clients now targeted with malware. The customers of Stratfor, a U.S.-based research group that provides geopolitical analysis to government organizations and major corporations, are being targeted again with malicious spam e-mails. Following the December breach of the company's servers by Anonymous and the stealing of names, home addresses, credit card details, and passwords of its clients, those very clients began to receive spear-phishing e-mails purportedly being sent by Stratfor's CEO, asking them to fill out an attached document with

personal information. This time, the e-mails appear to be sent by a Stratfor administrator, who first warns clients not to open e-mails and attachments from "doubtful senders," and then urges them to download (attached) security software to check their systems for a nonexistent piece of malware. "The link displayed in the emails appears legitimate at first glance, but looking closely at the target address, you notice that it doesn't originate from the address in the email text," according to Microsoft. "Stratfor is based in Texas, United States however the download URL is located somewhere in Turkey. A sample of another PDF file contained a download link for yet another compromised site, this time in Poland." Less careful users will end up with a malicious PDF file or a variant of the Zbot information stealer trojan on their systems. Source: http://www.net-security.org/malware_news.php?id=1996

(Utah) **Man charged in assassination plot of Utah governor.** A Utah man who police said threatened to assassinate the governor of Utah and conducted surveillance on the governor's mansion is facing multiple felony charges, the Associated Press reported February 12. The suspect was charged February 10 in Salt Lake City with felony counts of drug and weapons possession, along with a misdemeanor count of threatening elected officials. The man sent text messages to a friend February 2 stating that he was in the bushes and intended to kill the governor, court records said. The recipient of the texts reported the messages to police, and the suspect was arrested the same day. The texts also included a threat to kill a police officer who had driven past the mansion more than once during the suspect's period of surveillance. Police also said the governor was at home during the time the man was conducting surveillance and was removed from the premises for safety reasons. Investigators enlisted the help of the message recipient to get him to come to a nearby gas station, where he was arrested. Police found containers of ammunition, a large knife, explosives, illegal fireworks, and small plastic bags of methamphetamine in the suspect's truck. Security camera video from the area around the mansion also showed him conducting his surveillance. Source: http://www.huffingtonpost.com/2012/02/13/gary-herbert-utah-governor-assassination-brian-biff-baker_n_1272870.html?1329141901&ncid=edlinkusaolp00000008

Anonymous reverse ferrets on CIA.gov takedown. Hacking collective Anonymous claimed responsibility for making the CIA's Web site inaccessible February 10, but later said it was just reporting the event, The Register reported February 13. The apparent distributed denial of service attack against the agency's Web presence follows a week after the release of a recording of a conference call between FBI and British law enforcement officials discussing the progress of various cases against alleged members of Anonymous and LulzSec. A Twitter account associated with the activists' movement claimed credit for the takedown before backtracking and saying it was merely "noting" the cia.gov site was inaccessible. The conflicting statements created confusion about the cause of the outage. A CIA representative confirmed problems with the agency's site without commenting on the reasons for the downtime. The site returned to normal operation February 11. The site (which essentially serves as an online brochure for the agency and an outlet for public relations material) has been the target of hacktivists in the past, including a June 2011 attack by LulzSec. Source: http://www.theregister.co.uk/2012/02/13/cia_website_outage/

Uzbek national pleads guilty to plotting to kill the U.S. President on terror charges. An Uzbek national pleaded guilty in federal court February 10 to trying to kill the U.S. President and to supporting an Uzbek terror group. The man, who has been in the United States since overstaying a student visa in 2009, pleaded guilty to charges of threatening to kill the President, possession of an illegal weapon, and supporting the Islamic Movement of Uzbekistan, which is a U.S.-designated terror group. He was living in the Birmingham, Alabama, areas when he was indicted by a federal grand jury on the Presidential threat and terror charges in July 2011 after he tried to obtain an automatic weapon to kill the President in a federal undercover operation spurred by confidential informants. He faces maximum prison sentences of 15 years on the terrorism charge, 5 years on the charge of threatening the President, and 10 years on the charge of being an illegal alien in possession of a firearm. Each charge also carries a maximum fine of $250,000. Source:
http://www.gsnmagazine.com/node/25624?c=federal_agencies_legislative

Information Technology and Telecommunications

Cyber criminals find new way to exploit old Office hole. Cyberattackers found a new way to take advantage of an old Microsoft Office hole. Symantec researchers noticed a specially crafted trojan that exploits a previously patched vulnerability. The attack occurs when a user opens up an e-mail that contains a Microsoft Word file with a malicious Dynamic Link Library file (DLL). "The exploit makes use of an ActiveX control embedded in a Word document file," a researcher at Symantec said. "When the Word document is opened, the ActiveX control calls fputlsat.dll which has the identical file name as the legitimate .dll file used for the Microsoft Office FrontPage Client Utility Library." He said once this flaw is exploited, an attacker is free to load up an infected system with malware. He also advises that if a user sees an e-mail attachment with the file name ftutlsat.dll, proceed with caution. An e-mail with this type of attachment should be easy to spot, according to the researcher. The exploit, recently seen in the wild by the security firm, was previously fixed by Microsoft in September's Security Update, bulletin MS11-073. The researcher warns that because the bulletin was only classified as "important" by Microsoft, it might have been overlooked. Source:
http://gcn.com/articles/2012/02/10/trojan-exploits-unpatched-office-vulnerability.aspx

Waledac Botnet returns, steals passwords and credentials. In 2010, Microsoft was able to terminate the activity of the Waledac botnet, which at the time was famous for being a large source of spam. However, Palo Alto Networks researchers came across a new variant which is not only used for spamming, but also for stealing sensitive data from infected devices. The new version was spotted February 2. Experts conclude it is still sending spam, but it can also steal passwords and authentication data, including credentials for FTP, POP3, SMTP. Besides this, Waledac also steals .dat files for FTP and BitCoin and uploads them to the botnet. By relying on their WildFire systems, which enable a firewall to capture unknown files and analyze them in a malware sandbox, Palo Alto Networks was able to identify how the new variant behaves. Given the confusion created around the Kelihos botnet that was declared resurrected by Kaspersky, only to be put to sleep again by Microsoft, the company emphasizes this is not the old botnet,

but a new variant. Source: http://news.softpedia.com/news/Waledac-Botnet-Returns-Steals-Passwords-and-Credentials-253071.shtml

Researchers crack online encryption system. An online encryption method widely used to protect banking, e-mail, e-commerce, and other sensitive Internet transactions is not as secure as assumed, according to a report issued by a team of U.S and European cryptanalysts. The researchers reviewed millions of public keys used by Web sites to encrypt online transactions and found a small but significant number to be vulnerable. In most cases, the problem had to do with the manner in which the keys were generated, according to the researchers. The numbers associated with the keys were not always as random as needed, the research showed. Therefore, the team concluded, attackers could use public keys to guess the corresponding private keys that are used to decrypt data — a scenario previously believed to be impossible. Source: http://www.computerworld.com/s/article/9224265/Researchers_crack_online_encryption_system?taxonomyId=17

Horde FTP server hacked, files maliciously altered. The developers of the popular open source Web mail solution Horde identified a number of manipulated files on an FTP server. They concluded the server was breached, the files stored on it being altered to allow unauthenticated remote PHP execution. "We have immediately taken down all distribution servers to further analyze the extent of this incident, and we have worked closely with various Linux distributions to coordinate our response," Horde officials said. After the investigation was concluded, the servers were replaced and secured, and the altered files replaced with clean variants. The analysis found three files were manipulated and modified on different occasions, and served to unsuspecting customers for about 3 months. Horde 3.3.12 was manipulated November 15, 2011, Horde Groupware 1.2.10 November 9, 2011, and Horde Groupware Webmail Edition 1.2.10 November 2, 2011. Since the incident was found February 7, users who downloaded the files during this timeframe are advised to immediately reinstall using fresh copies from Horde's FTP server, or upgrade to more recent versions that have been released since. Horde 4 releases were not affected and neither were the company's CVSs and Git repositories. The affected Linux distributions will provide notifications and security updates of their own. Users who are uncertain if they are exposed to cybercriminal operations can manually verify whether or not their products were altered by searching for the $m[1]($m[2]) signature in the Horde directory tree. Source: http://news.softpedia.com/news/Horde-FTP-Server-Hacked-Files-Maliciously-Altered-252708.shtml

Twitter turns on HTTPS by default. Twitter recently turned HTTPS on by default for all users. The option to always use HTTPS was made available to users in March 2011, but they had to turn it on for themselves by changing their account settings. Twitter's very nature and the fact that many users are used to tweeting from unsecured Internet connections meant anyone equipped with the Firesheep Firefox add-on can easily steal their log-in credentials sent via unencrypted HTTP sessions. Source: http://www.net-security.org/secworld.php?id=12396

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

Roche warns of counterfeit Avastin in U.S. The maker of the best-selling anticancer drug Avastin is warning doctors and patients about counterfeit vials of the product distributed in the United States, the Associated Press reported February 14. Roche's Genentech unit said the fake products do not contain the key ingredient in Avastin, which is used to treat cancers of the colon, lung, kidney, and brain. The company believes drugs labeled with the following lot numbers may be fake: B86017, B6011, and B6010. The counterfeit products do not have "Genentech" printed on their packaging, which appears on all FDA-approved cartons and vials. A spokeswoman said the counterfeit drug was distributed to health care facilities in the United States. The company is working with the Food and Drug Administration to track down the counterfeit vials and analyze their contents. It said it was alerted to the problem by foreign health regulators and believes the counterfeits were imported from abroad. Additionally, legitimate Avastin contains a six-digit lot number with no letters. All the text on the product's packaging is in English. Source: http://yourlife.usatoday.com/health/story/2012-02-14/Roche-warns-of-counterfeit-Avastin-in-US/53096312/1

FDA investigating illegal online sale of handheld dental x-ray units. The U.S Food and Drug Administration (FDA) is warning dental and veterinary professionals to not purchase or use certain potentially unsafe hand-held dental X-ray units. The FDA is concerned these devices may not be safe or effective, and could expose the user and the patient to unnecessary and potentially harmful X-rays. The units, sold online by manufacturers outside the United States and directly shipped to U.S. customers, have not been reviewed by the FDA and do not meet FDA radiation safety requirements. The Washington State Department of Health alerted the FDA after tests on a device purchased online revealed it did not comply with X-ray performance standards. All X-ray units that have been cleared by the FDA bear a permanent certification label/tag, a warning label, and an identification label/tag on the unit. Source: http://www.prnewswire.com/news-releases/fda-investigating-illegal-online-sale-of-handheld-dental-x-ray-units-139093199.html

Transportation

Nothing Significant to Report

Water and Dams

Nationwide radium testing of groundwater shows most susceptible regions are central U.S. and East Coast. According to a study conducted by the U.S. Geological Survey (USGS), groundwater in aquifers on the East Coast and in the central United States have the highest risk of contamination from radium, a naturally occurring radioactive element and known carcinogen. Radium was detected in concentrations that equaled or exceeded U.S. Environmental Protection Agency (EPA) drinking water standards in more than one in five wells tested in the Mid-Continent and Ozark Plateau Cambro-Ordovician aquifer systems, underlying parts of Arkansas, Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, and Wisconsin; and the North Atlantic Coastal Plain aquifer system, underlying parts of Delaware, Maryland, New Jersey, New York, North Carolina, and Virginia. The study found that if the groundwater has low oxygen or low pH, radium is more likely to dissolve and become present. Low oxygen conditions were prevalent in the Mid-Continent and Ozark Plateau Cambro-Ordovician aquifer systems, and low pH conditions were prevalent in the North Atlantic Coastal Plain aquifer system. In most aquifers used for drinking water, radium concentrations were below EPA standards, especially in the West. Source: http://www.usgs.gov/newsroom/article.asp?ID=3104

(Ohio) **EPA begins testing sites for contamination.** The U.S. Environmental Protection Agency (EPA) began testing 14 sites in Sandusky County, Ohio, February 13 for possible contamination, a study spurred by a high number of childhood cancer cases in the area. Since the mid-1990s, at least 35 children in a 12-mile radius in the east half of the county have been diagnosed with various types of cancer. Four have died. The study may not find the root cause of the cluster, but any contamination it does uncover would still help the community, said the county administrator whose 11-year daughter, died of cancer in 2009. The sites, many of which are former dumps, were determined as possible areas of contamination by a 2009 study of the cancer cluster. Crews will take soil, water and gas samples from the ground at each site, a process expected to take 2-3 weeks. After the samples are tested and analyzed, the EPA expects to report any findings in the late spring or early summer. Source: http://www.thenews-messenger.com/article/20120213/NEWS01/120213007/EPA-begins-testing-sites-contamination

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168